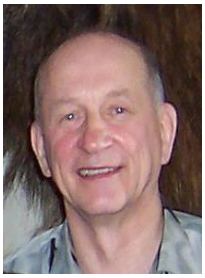
ОБРАБОТКА ИЗОБРАЖЕНИЙ И РАСПОЗНАВАНИЕ ОБРАЗОВ

УДК 621.391

В.Г. Лабунец[1], В.П. Часовских[1], Е.Остхаймер[2]

[1]Уральский государственный лесотехнический университет, г. Екатеринбург
[2]Capricat LLC 1340 S. Ocean Blvd., Suite 209 Pompano Beach, 33062 Florida, USA

КРИПТОСИСТЕМЫ, ОСНОВАННЫЕ НА РС- И БЧХ-КОДАХ НАД НЕКОММУТАТИВНЫМИ АЛГЕБРАМИ



Ключевые слова: *симметричные криптосистемы, РС-коды, БЧХ-коды, алгебры клиффорда, алгебры Кэли-Диксона, преобразования Фурье-Галуа-Клиффорда со связкой ключей.*

В данной работе мы вводим в рассмотрение новые криптосистемы, основанные на РС- и БЧХ-кодах и преобразованиях Фурье-Галуа-Клиффорда, оснащенных связками ключей.

V.G. Labunets[1], V.P. Chasovskikh[1], E.Osthaimer[2]

[1]Ural State Forest Engineering University, Sibirsky trakt, 37, Ekaterinburg, Russia, 620100
[2]Capricat LLC, Pompano Beach, Florida, USA

CRYPTOSYSTEMS BASED ON RS AND BCH CODES OVER FINITE NONCOMMUTATIVE ALGEBRAS

Keywords: symmetric cryptosystems**,** *Reed-Solomon codes, Bose-Chaudhuri-Hocquenghem codes, Clifford algebra, Cayley-Dickson algebra, Fourier-Galois-Clifford transforms.*

The purpose of this paper is to introduce new cryptosystems based on linear Reed-Solomon (RC) and Bose-Chaudhuri-Hocquenghem (BCH) codes over finite *Cayley-Dickson and finite* Clifford algebras with fast code and encode procedures based on fast Fourier-Clifford-Galois and *Fourier- Cayley-Dickson-Galois* transforms

---

Лабунец Валерий Григорьевич – доктор технических наук, профессор, заслуженный работник высшей школы РФ, профессор кафедры теоретических основ радиотехники Уральского федерального университета (Екатеринбург). Тел.: +7-953-383-37-64; e-mail: vlabunets@yahoo.com.

Labunets Valery Grigor'evch– Doctor of technical sciences, Professor, Ural Federal University (Yekaterinburg). Phone: +7-953-383-37-64; e-mail: vlabunets05@yahoo.com

Часовских Виктор Петрович - доктор технических наук, профессор, заслуженный работник высшей школы РФ, член Российской академии инженерных наук им. А.М. Прохорова, член Российской академии естественных наук, FullMemberofEuropeanAcademyofNaturalHistory, директор Института экономики и

управления Уральского государственного лесотехнического университета (Екатеринбург). Тел. (343)261-46-44; e-mail: u2007u@ya.ru.

Chasovskikh Viktor Petrovich - Doctor of technical sciences, Professor, Director of the Institute of Economics and Management, Ural State Forest Engineering University (Yekaterinburg). Phone: (343)261-46-44; e-mail: u2007u@ya.ru.

Остхаймер Екатерина – доктор философии по компьютерным наукам, директор фирмы CapricatLLC (Флорида, США). Тел.: +7-953-383-37-64; e-mail: katya@capricat.com

Osthaimer Ekaterina - Doctor of Philosophy in Computer Science, Director of Capricat LLC (Pompano Beach 33062 Florida USA). Phone: +7-953-383-37-64; e-mail:katya@capricat.com

---

1. Introduction

The idea of public key cryptography (PKC) was introduced by W. Diffie and M.E. Hellman (Diffie, Hellman, 1976) in 1976. Today, most succusseful PKC-schemes are based on the perceived difficulty of certain problems in particular large finite commutative rings. For example, the difficulty of solving the integer factoring problem (IFP) defined over the ring $\mathbf{Z}_m$ (where m is the product of two large primes) forms the ground of the basic RSA cryptosystem (Cao, 1999, 2000, 2001; Komaya et al., 1992; Rabin, 1979; Rackoff, Simon, 1992; Rivest et al., 1978; Smith, Lennon, 1993; Williams, 1980, 1985). The extended multi-dimension RSA cryptosystem (Cao, 2000), which can efficiently resist low exponent attacks, is also defined over the commutative ring $\mathbf{Z}_m[X]$.

Currently there are many attempts to develop alternative PKC based on different kinds of problems on noncommutative algebraic structures. The most researchers use non-commutative groups as a good alternative platform for constructing public-key cryptosystems: braid groups; (Anshel et al., 1999; Bohli et al., 2006; Dehornoy, 2004; Ko et al., 2000), poly-cyclic groups (Anshel et al., 1999; Bohli et al., 2006; Dehornoy, 2004; Ko et al., 2000), Thompson's groups (Eick, Kahrobaei, 2004; Paeng et al., 2001; Shpilrain, Ushakov, 2005).

In this paper, we would like to propose a new method for designing public key cryptosystems based on RS and BCH codes over finite *Cayley-Dickson and finite* Clifford algebras. The key idea of our proposal is that for a given non-commutative algebra, we can define polynomials and take them as the underlying work structure in order to do decoding as NP-hard *for the family of Reed-Solomon codes* over noncommutative algebras.

The rest of the paper is organized as follows: in Section 2, the object of the study (Reed-Solomon and Bose-Chaudhuri-Hocquenghem codes) is described. In Section 3, the proposed method based on noncommutative algebras is explained.

2. The object of the study. Reed-Solomon and Bose-Chaudhuri-Hocquenghem codes

The Bose, Chaudhuri and Hocquenghem (BCH) codes are sub class of cyclic codes. Binary BCH codes were discovered by Hocquenghem in 1959 and independently by Bose and Chaudhuri in 1960. The Reed-Solomon (RS) Code is an important subset of the non-binary BCH Codes. In 1960, Irving Reed and Gus Solomon published a paper in the *Journal of the Society for Industrial and Applied Mathematics* (Reed, Solomon, 1960). This paper described a new class of error-correcting codes that are now called *Reed-Solomon* (R-S) *codes*. These codes have great power and utility, and are today found in many applications in the intelligent communication systems, cognitive radio systems and in various technical communication standards like the *Consultative Committee for Space Data Systems* (CCSDS) Telemetry channel coding standard, the Digital Video Broadcasting (DVB) standards as well as in the *Digital Subscriber Line* (DSL) standard. Historically, RS codes were introduced by Reed and Solo-

mon as valuation codes. In the 1960s and 1970s, RS and BCH codes were primarily studied as cyclic codes. The transform approach was popularized by Blahut in the early 1980s.

In order to understand the encoding and decoding principles of Reed-Solomon (R-S) codes, it is necessary to venture into the area of finite fields known as *Galois Fields* (GF). For any prime number, p, there exists a finite field denoted GF(p) that contains p elements. It is possible to extend GF(p) to a field of p^m elements, called an *extension field* of GF(p), and denoted by $\mathrm{GF}(q) := \mathrm{GF}(p^m)$, where m is a nonzero positive integer. Note that commutative Galois field $\mathrm{GF}(p^m)$ contains as a subset the elements of GF(p). Symbols from the extension field $\mathrm{GF}(p^m)$ are used in the construction of classical Reed-Solomon (R-S) codes.

An (n,k) linear code $Cod(n,k\,|\,\mathrm{GF}(q))$ is k D subspace of the vector space $\mathrm{GF}^n(q)$ of all n-tuples $\mathbf{c} = (c_0, c_1, ..., c_{n-1})$ over GF(q), *i.e.*, $Cod(n,k\,|\,\mathrm{GF}(q)) \subset \mathrm{GF}^n(q)$. Any k linearly independent codewords $(g_0, g_1, ..., g_{n-1})$ generate $Cod(n,k\,|\,\mathrm{GF}(q))$, in the sense that

$$Cod(n,k\,|\,\mathrm{GF}(q)) = \left\{ \sum_{j=1}^{k} a_j \mathbf{g}_j \,\middle|\, \forall a_j \in \mathrm{GF}(q) \right\}.$$

Thus $Cod(n,k\,|\,\mathrm{GF}(q))$ has q^k distinct codewords.

Reed-Solomon (RS) codes are *nonbinary cyclic* codes with symbols made up of m-bit sequences, where m is any positive integer having a value greater than 2. RS(n,k) codes on m-bit symbols exist for all n and k for which $0 < k < n < 2^m + 2$, where k is the number of data symbols being encoded, and n is the total number of code symbols in the encoded block. For the most conventional RS(n,k) code, $(n,k) = (2^m - 1, 2^m - 1 - 2t)$, where t is the symbol-error correcting capability of the code, and $n - k = 2t$ is the number of parity symbols. Reed-Solomon codes achieve the *largest possible* code minimum distance for any linear code with the same encoder input and output block lengths. For Reed- Solomon codes, the code minimum distance is given by [2] $d_{\min} = n - k + 1 = 2t + 1$. The most natural definition of RS code is in terms of a certain evaluation map from the subspace $\mathrm{GF}^k(q)$ of all n-tuples $\mathbf{m} = (m_0, m_1, ..., m_{k-1})$ (information symbols (massage)) over GF(q) to the set of codewords $Cod(n,k\,|\,\mathrm{GF}(q)) \subset \mathrm{GF}^n(q)$:

$$\mathbf{m} = (m_0, m_1, ..., m_{k-1}) \mapsto \mathbf{c} = (c_0, c_1, ..., c_{n-1}), \quad \mathrm{GF}^k(q) \to \mathrm{GF}^n(q) \tag{1}$$

Definition 1. Let GF(q) be a finite field and GF(q)[X] denote the GF(q)-space of univariate polynomials where all the coefficients of X are from GF(q). Pick $D = \{\beta_0, \beta_1, ..., \beta_{n-1}\}$ n different elements of GF(q) arranged in some arbitrary order and choose n and k such that $k \le n \le q - 1$. The most convenient arrangement is $\beta_0 = \varepsilon^b, \beta_1 = \varepsilon^{b+1}, ..., \beta_i = \varepsilon^{b+i}, ..., \beta_{n-1} = \varepsilon^{b+n-1}$ for a some integer $b + k \le q - 2$, where ε is a primitive element of GF(q). We define an encoding function for Reed-Solomon code as $\mathrm{RS}: \mathrm{GF}^k(q) \to \mathrm{GF}^n(q)$ in the following form. A message $\mathbf{m} = (m_0, m_1, ..., m_{k-1})$ with $m_i \in \mathrm{GF}(q)$ is mapped to a degree $k-1$ polynomial (it is called the information polynomial in the indeterminate X):

$$f_{\mathbf{m}}(X) = m_0 X^0 + m_1 X^1 + ... + m_{k-1} X^{k-1} = \sum_{j=0}^{k-1} m_j X^j. \tag{2}$$

Obviously, $f_{\mathbf{m}}(X)$ is one of the q^k polynomials over GF(q) of degree less than k. The information polynomial $f_{\mathbf{m}}(X)$ is then mapped into the n-tuple $\left(f_{\mathbf{m}}(\beta_0), f_{\mathbf{m}}(\beta_1), ..., f_{\mathbf{m}}(\beta_{n-1})\right)$, i.e.,

$$\mathbf{m} = (m_0, m_1, ..., m_{k-1}) \to f_{\mathbf{m}}(X) \to \left(f_{\mathbf{m}}(\beta_0), f_{\mathbf{m}}(\beta_1), ..., f_{\mathbf{m}}(\beta_i), ..., f_{\mathbf{m}}(\beta_{n-1}) \right),$$

whose components $f_{\mathbf{m}}(\beta_i)$ are equal to the evaluations of the polynomials $f_{\mathbf{m}}(X)$ at each field element $\beta_i \in \mathrm{GF}(p)$:

$$f_{\mathbf{m}}(\beta_i) = m_0\beta_i^0 + m_1\beta_i^1 + ... + m_{k-1}\beta_i^{k-1} = \sum_{j=0}^{k-1} m_j \beta_i^j, \quad 0 \le i \le n-1, \tag{3}$$

$$f_{\mathbf{m}}(\beta_i) = m_0\beta_i^0 + m_1\beta_i^1 + ... + m_{k-1}\beta_i^{k-1} = \sum_{j=0}^{k-1} m_j \beta_i^j, \quad 0 \le i \le n-1,$$

or

$$f_{\mathbf{m}}(\beta_i) = f_{\mathbf{m}}(\varepsilon^{b+i}) = m_0\varepsilon^{(b+i)0} + m_1\varepsilon^{(b+i)1} + ... + m_{k-1}\varepsilon^{(b+i)(k-1)} = \sum_{j=0}^{k-1} m_j \varepsilon^{(b+i)j}, \quad 0 \le i \le q-2, \tag{4}$$

for a common special case $\beta_0 = \varepsilon^b, \beta_1 = \varepsilon^{b+1}, ..., \beta_i = \varepsilon^{b+i}, ..., \beta_{n-1} = \varepsilon^{b+n-2}$ and $n = q-1$. The code generators may thus as polynomials

$$\begin{aligned}
\mathbf{g}_0 &= \left(1,\ \varepsilon^{(b+0)\cdot 1},\ \varepsilon^{(b+0)\cdot 2},\ ...,\ \varepsilon^{(b+0)\cdot(n-1)}\right),\\
\mathbf{g}_1 &= \left(1,\ \varepsilon^{(b+1)\cdot 1},\ \varepsilon^{(b+1)\cdot 2},\ ...,\ \varepsilon^{(b+1)\cdot(n-1)}\right),\\
\mathbf{g}_2 &= \left(1,\ \varepsilon^{(b+2)\cdot 1},\ \varepsilon^{(b+2)\cdot 2},\ ...,\ \varepsilon^{(b+2)\cdot(n-1)}\right),\\
&... \qquad .....,\\
\mathbf{g}_{k-1} &= \left(1, \varepsilon^{(b+k-1)\cdot 1}, \varepsilon^{(b+k-1)\cdot 2}, ..., \varepsilon^{(b+k-1)\cdot(n-1)}\right).
\end{aligned}$$

Hence, generator matrix for RS codes is the *VanDerMonde* matrix with $n \times k$ size

$$\begin{bmatrix}
1 & 1 & ... & 1 \\
\varepsilon^{1\cdot(b+0)} & \varepsilon^{1\cdot(b+1)} & ... & \varepsilon^{1\cdot(b+k-1)} \\
... & ... & ... & ... \\
\varepsilon^{(n-1)\cdot(b+0)} & \varepsilon^{(n-1)\cdot(b+1)} & ... & \varepsilon^{(n-1)\cdot(b+k-1)}
\end{bmatrix}$$

and encoding a message block $\mathbf{m} = (m_0, m_1, ..., m_{k-1})$ via the evaluation map in (4) is equivalent to computing the Fourier-Galois Transform of the n-tuple $(0, ..., 0, m_{b+0}, m_{b+1}, ..., m_{b+k-1}, 0, ..., 0)$:

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ ... \\ ... \\ c_i \\ ... \\ ... \\ c_{n-2} \\ c_{n-1} \end{bmatrix} = \left[\begin{array}{ccc|ccc|ccc}
1 & 1 & ... & 1 & 1 & ... & 1 & 1 & ... \\
1 & \varepsilon^{1\cdot 1} & ... & \varepsilon^{1\cdot(b+0)} & \varepsilon^{1\cdot(b+1)} & ... & \varepsilon^{1\cdot(b+k-1)} & \varepsilon^{1\cdot(b+k)} & ... \\
1 & \varepsilon^{2\cdot 1} & ... & \varepsilon^{2\cdot(b+0)} & \varepsilon^{2\cdot(b+1)} & ... & \varepsilon^{2\cdot(b+k-1)} & \varepsilon^{2\cdot(b+k)} & ... \\
... & ... & ... & ... & ... & ... & ... & ... & ... \\
... & ... & ... & ... & .... & ... & ... & ... & .... \\
1 & \varepsilon^{i\cdot 1} & ... & \varepsilon^{i\cdot(b+0)} & \varepsilon^{i\cdot(b+1)} & ... & \varepsilon^{i\cdot(b+k-1)} & \varepsilon^{i\cdot(b+k)} & ... \\
... & ... & ... & ... & ... & ... & .... & ... & ... \\
... & ... & ... & ... & ... & ... & .... & ... & ... \\
1 & \varepsilon^{(n-2)\cdot 1} & ... & \varepsilon^{(n-2)\cdot(b+0)} & \varepsilon^{(n-2)\cdot(b+1)} & ... & \varepsilon^{(n-2)\cdot(b+k-1)} & \varepsilon^{(n-2)\cdot(b+k)} & ... \\
1 & \varepsilon^{(n-1)\cdot 1} & ... & \varepsilon^{(n-1)\cdot(b+0)} & \varepsilon^{(n-1)\cdot(b+1)} & ... & \varepsilon^{(n-1)\cdot(b+k-1)} & \varepsilon^{(n-1)\cdot(b+k)} & ...
\end{array}\right] \begin{bmatrix} 0 \\ ... \\ 0 \\ m_{b+0} \\ m_{b+1} \\ \cdots \\ m_{b+k-1} \\ 0 \\ \cdots \\ 0 \end{bmatrix}$$

A codewords has a zero symbols in the coordinate corresponding to β_i if and only if $f_{\mathbf{m}}(\beta_i) = 0$; *i.e.*, if and only if β_i is a root of equation $f_{\mathbf{m}}(X) = 0$. By the fundamental theorem of algebra if $\deg\{f_{\mathbf{m}}(X)\} \le k-1$ then equation $f_{\mathbf{m}}(X) = 0$ can have at most $k-1$ roots in $\mathrm{GF}(q)$.

3. Methods

In this section we describe a construction technique of BCH and RS codes over finite noncommutative algebras in order to prove that maximum-likelihood decoding is NP-hard *for the family of Reed-Solomon codes* over noncommutative algebras. There are noncommutative extensions of $\mathrm{GF}(p)$ in the form of Clifford or Cayley-Dickson algebras of p^m elements

$$Cl_m(p) = ClifAlg_m\{i_1, i_2, ..., i_s \mid \mathbf{GF}(p)\}, \quad CD_m(p) = CayDicAlg_m\{i_1, i_2, ..., i_s \mid \mathbf{GF}(p)\}.$$

Let us denote $Alg_m(p) = Cl_m(p),\ CD_m(p)$, where $m = q^s$ for any prime number q and a nonzero positive integer s. Symbols from the Clifford or Cayley-Dickson algebras $Alg_m(p)$ (instead of symbols from the extension field $\mathrm{GF}(p^m)$) we are going to use in the construction of generalized Reed-Solomon codes.

3.1.Reed-Solomon and Bose codes over noncommutative algebras

Let X be a formal noncommutative variable with respect to elements $a \in Alg_{2^m}(p)$, *i.e.*, $aX \neq Xa$ and let X be its k^{th} degree. We introduce new notion of monomial $X^{k,[\sigma]}$ with key $[\sigma]$ by $X^{k,[\sigma]} = X^{\sigma} \underset{\sigma}{(\circ)} X^{k-\sigma} = \underbrace{X \cdot X \cdot ... \cdot X}_{\sigma} \underset{\sigma}{(\circ)} \underbrace{X \cdot X \cdot ... \cdot X}_{k-\sigma}$ and introduce two noncommutative products with one key $[\sigma]$:

$$a(X) := \begin{cases} a \cdot X^{[\sigma]}, & \sigma = 0, \\ X^{[\sigma]} \cdot a, & \sigma = 1 \end{cases} \qquad a \cdot X^{k,[\sigma_k]} := X^{\sigma} \cdot a \cdot X^{k-\sigma}, \quad \text{for} \quad \sigma^k = \mathbf{Z}_k = \{0,1,...,k\}.$$

For example,

$$a \cdot X^{3,[0]} := X^0 \cdot a \cdot X^3, \quad a \cdot X^{3,[1]} := X^1 \cdot a \cdot X^2,$$
$$a \cdot X^{3,[2]} := X^2 \cdot a \cdot X^1, \quad a \cdot X^{3,[3]} := X^3 \cdot a \cdot X^0.$$

For commutative algebras $a \cdot X^{3,[0]} = a \cdot X^{3,[1]} = a \cdot X^{3,[2]} = a \cdot X^{3,[3]}$, since $X^0 \cdot a \cdot X^3 = X^1 \cdot a \cdot X^2 = X^2 \cdot a \cdot X^1 = X^3 \cdot a \cdot X^0$, but $a \cdot X^{3,[0]} \neq a \cdot X^{3,[1]} \neq a \cdot X^{3,[2]} \neq a \cdot X^{3,[3]}$, for noncommutative algebras, since $X^0 \cdot a \cdot X^3 = X^0 \cdot a \cdot X^1 \neq X^1 \cdot a \cdot X^2 \neq X^2 \cdot a \cdot X^1 \neq X^3 \cdot a \cdot X^0$.
Now, let

$$f^{[\boldsymbol{\sigma}]}(X) = f^{[(\sigma_0, \sigma_1, ..., \sigma_{n-1})]}(X) = \sum_{i=0}^{n-1} a_i X^{i,[\sigma_i]} = \sum_{i=0}^{n-1} X^{\sigma_i} a_i X^{i-\sigma_i},$$

be polynomials with a bunch of keys. There are $n! = 1 \cdot 2 \cdot 3 \cdots n$ similar bunch of keys $\boldsymbol{\sigma} = (\sigma_0, \sigma_1, ..., \sigma_{n-1})$.

Example 1. For $\boldsymbol{\sigma} = (0,0,...,0)$ and $\boldsymbol{\sigma} = (0,1,2,3,...,n-1)$ we have right- and left-side polynomials

$$f^{[(0,0,...,0)]}(X) = f^{l}(X) = \sum_{i=0}^{n-1} a_i X^{i,[0]} = \sum_{i=0}^{n-1} a_i \cdot X^i,$$
$$f^{[(0,1,2,...,n-1)]}(X) = {}^{r}f(X) = \sum_{i=0}^{n-1} a_i X^{i,[i]} = \sum_{i=0}^{n-1} X^i \cdot a_i.$$

Let

$$Alg_{2^m}^{[\boldsymbol{\sigma}]}(p)[X] = Alg_{2^m}^{[(\sigma_0, \sigma_1, ..., \sigma_{n-1})]}(p)[X] :=$$
$$= \left\{ f^{[\boldsymbol{\sigma}]}(X) = \sum_{i=0}^{n-1} a_i X^{i,[\sigma_i]} \mid \left(\forall a_i \in Alg_{2^m}(p)\right) \& \left(\boldsymbol{\sigma} \in \mathrm{Z}_n\right) \right\},$$

denote the rings of univariate polynomials over $Alg_{2^m}(p)$ with a bunch of keys $\boldsymbol{\sigma}=(\sigma_0,\sigma_1,...,\sigma_{n-1})$.

Reed-Solomon codes with the bunch of keys $\boldsymbol{\sigma}=(\sigma_0,\sigma_1,...,\sigma_{n-1})$ are obtained by evaluating certain subspaces of $Alg_{2^m}^{[\boldsymbol{\sigma}]}(p)[X]$ in set of points $D=\{x_0,x_1,...,x_{n-1}\}$ which are a subsets of $Alg_{2^m}(p)$. Specifically, a Reed-Solomon codes $Code\left\{D,k\mid f^{[\boldsymbol{\sigma}]}(X),Alg_{2^m}(p)\right\}$ of length n and dimension k over $Alg_{2^m}(p)$ are defined as follows:

$$Code^{(l)}\left\{D,k\mid f^{[\boldsymbol{\sigma}]}(X),Alg_{2^m}(p)\right\}:=$$

$$=\left\{\left(f^{[\boldsymbol{\sigma}]}(x_0),f^{[\boldsymbol{\sigma}]}(x_1),...,f^{[\boldsymbol{\sigma}]}(x_{n-1})\right)\mid\left(f^{[\boldsymbol{\sigma}]}(X)\in Alg_{2^m}^{[\boldsymbol{\sigma}]}(p)[X]\right)\&\left(\deg\left\{f^{[\boldsymbol{\sigma}]}(X)\right\}<k\right)\right\}.$$

Thus a Reed-Solomon code is completely specified in terms of its evaluation set $D=\{x_1,x_2,...,x_n\}$ and its dimension k.

We assume that if a codeword $\mathbf{s}\in Code\left\{D,k\mid f^{[\boldsymbol{\sigma}]}(X),Alg_{2^m}(p)\right\}$ of is transmitted and the vector $\mathbf{y}\in Alg_{2^m}^n(p)$ is received, the maximum-likelihood decoding task consists of computing a codeword $\mathbf{v}\in Code\left\{D,k\mid f^{[\boldsymbol{\sigma}]}(X),Alg_{2^m}(p)\right\}$ that minimizes $d(\mathbf{s},\mathbf{v})$, where $d(\cdot,\cdot)$ denotes the Hamming distance. The corresponding decision problem can be formally stated as follows. We let c_i be the codeword symbols, where i runs from 0 to $n-1$, *i.e.*,

$$(c_0,c_1,...,c_{n-1})=\left(f^{[\boldsymbol{\sigma}]}(x_0),f^{[\boldsymbol{\sigma}]}(x_1),...,f^{[\boldsymbol{\sigma}]}(x_{n-1})\right) \tag{5}$$

and let u_k be the information symbols, where k runs from 0 to $k-1$. An RS coding procedures can then be defined by relating c_i to u_k according to

$$c_j=f^{[\boldsymbol{\sigma}]}(x_j)=\sum_{i=0}^{k-1}u_i\,x_j^{i,[\sigma_i]}=\sum_{i=0}^{k-1}x_j^{\sigma_i}\cdot u_i\,x_j^{i-\sigma_i}$$

or in matrix form

$$\begin{bmatrix}c_0\\c_1\\...\\c_{n-1}\end{bmatrix}=\begin{bmatrix}x_0^{0,\sigma_0}&x_0^{1,\sigma_1}&...&x_0^{k-1,\sigma_{k-1}}\\x_1^{0,\sigma_0}&x_1^{1,\sigma_1}&...&x_1^{k-1,\sigma_{k-1}}\\...&...&...&...\\x_{n-1}^{0,\sigma_0}&x_{n-1}^{1,\sigma_1}&&x_{n-1}^{k-1,\sigma_{k-1}}\end{bmatrix}\begin{bmatrix}u_0\\u_1\\...\\u_{k-1}\end{bmatrix}=$$

$$=\begin{bmatrix}x_0^0(\circ)&x_0^{\sigma_1}\cdot(\circ)\cdot x_0^{1-\sigma_1}&...&x_0^{\sigma_{k-1}}\cdot(\circ)\cdot x_0^{k-\sigma_{k-1}}\\x_1^0(\circ)&x_1^{\sigma_1}\cdot(\circ)\cdot x_1^{1-\sigma_1}&...&x_1^{\sigma_{k-1}}\cdot(\circ)\cdot x_1^{k-\sigma_{k-1}}\\...&...&...&...\\x_{n-1}^0(\circ)&x_{n-1}^{\sigma_1}\cdot(\circ)\cdot x_{n-1}^{1-\sigma_1}&...&x_{n-1}^{\sigma_{k-1}}\cdot(\circ)\cdot x_{n-10}^{k-\sigma_{k-1}}\end{bmatrix}\begin{bmatrix}u_0\\u_1\\...\\u_{k-1}\end{bmatrix}.$$

These generator matrices have forms of discrete Vandermonde-Clifford-Galois transform (if $Alg_{2^m}(p)=Cl_{2^m}(p)$) or Vandermonde -Caley-Dickson-Galois (if $Alg_{2^m}(p)=CD_{2^m}(p)$) transform. If we define $\varepsilon\in Alg_{2^m}(p)$ to be a primitive element of power n (i.e., the powers of ε^j, where j runs from 1 to $n-1$, are all different from each other), then RS codes for $x_j=\varepsilon^{j-1}$ $(j=1,2,...,n)$ can then be defined as

$$c_j=f^{[\boldsymbol{\sigma}]}(x_j)\Big|_{x_j=\varepsilon^{j-1}}=f^{[(\sigma_0,\sigma_1,...,\sigma_{k-1})]}(\varepsilon^{j-1})=\sum_{i=1}^{k-1}\varepsilon^{\sigma_i(j-1)}\cdot u_i\cdot\varepsilon^{(i-\sigma_i)(j-1)},$$

This has the form of discrete Fourier-Clifford-Galois or Fourier-Caley-Dickson-Galois transforms (DFCGTs or DFCDGTs) over $Alg_{2^m}(p)$, where the k "frequency" components until (from d until $d+k-1$) are given by the information symbols $u_0, u_1, ..., u_{k-1}$, and the other $n-k$ frequency components are fixed to zero [5].

Example 2. For $\boldsymbol{\sigma} = (0,0,...,0)$ and $\boldsymbol{\sigma} = (0,1,2,3,...,n-1)$ we have right- and left-side transforms

$$c_j = f^{(r)}(x_j) = \sum_{i=1}^{k-1} \varepsilon_j^{i(j-1)} \cdot u_i, \quad c_j = f^{(l)}(x_j) = \sum_{i=1}^{k-1} u_i \cdot \varepsilon_j^{i(j-1)}.$$

These transforms can be viewed as polynomial evaluations (5). Since evaluating a polynomial at multiple points can be implemented as a DFT, DFTs can be used to reduce the encode computational complexity, if a bunch of keys is known. When $n = 2^l$, the Cooley-Tukey algorithm can be carried out.

4. Conclusions

According to Berlekamp, McEliece, and van Tilborg maximum-likelihood decoding of linear codes is NP-complete over all finite fields **GF**(p) .In this paper, we have shown a new unified approach to the Reed-Solomon and Bose-Chaudhuri-Hocquenghem codes over finite noncommutative algebras. The approach is based on a bunch of keys for discrete Fourier-Clifford-Galois or Fourier-Caley-Dickson-Galois transforms. Cardinality of the set of bunch of keys is equal to $k!$ for (n,k)-code.

Acknowledgment

This work was supported by grants the RFBR № 17-07-00886, № 17-29-03369 and by Ural State Forest Engineering's Center of Excellence in "Quantum and Classical Information Technologies for Remote Sensing Systems".

References

Anshel I., Anshel M., Goldfeld D. An algebraic method for public-key cryptography // Math. Research Letters. 1999. No 6. P. 287-291.

Bohli J.-M., Glas B. Steinwandt R. Towards provable secure group key agreement building on group theory // Cryptology ePrint Archive: Report 2006/079, 2006 (https://eprint.iacr.org/2006/079).

Cao Z. A threshold key escrow scheme based on public key cryptosystem // Science in China (E Series). 2001. Vol. 44. No 4. P. 441-448.

Cao Z. Conic analog of RSA cryptosystem and some improved RSA cryptosystems // Natural Science Journal of Heilongjiang University. 1999. Vol. 16. No 4. P. 5-18.

Cao Z. The multi-dimension RSA and its low exponent security // Science in China (E Series). 2000. Vol. 43. No 4. P. 349-354.

Dehornoy P. Braid-based cryptography // Contemporary Mathematics. 2004. Vol. 360. P. 5-33.

Diffie W., Hellman M.E. New directions in cryptography // IEEE Trans. Inform. Theory, 1976. Vol. 22. P. 644-654.

Eick B, Kahrobaei D. Polycyclic groups: a new platform for cryptography // Preprint arXiv: math.GR/0411077, 2004. P. 1-7.

Ko K.H., Lee S.J., Cheon J.H., Han J.W. et al. New Public-Key Cryptosystem Using Braid Groups // M.Bellare (ed.): CRYPTO 2000, LNCS 1880. Springer-Verlag, 2000. P. 166-183.

Komaya K., Maurer U., Okamoto T., Vanston S. Newpublic-key schemes bases on elliptic curves over the ring Z_n // J. Feigenbaum (ed.): Crypto'91, LNCS 576. Springer-Verlag, 1992. P. 252-266.

Paeng S.-H., Ha K.-C., Kim J.-H., Chee S., Park C. New public key cryptosystem using finite Non Abelian Groups // J. Kilian (ed.): CRYPTO 2001, LNCS 2139. Springer-Verlag, 2001. P. 470-485.

Rabin M.O. Digitized signatures and public-key functions as intractible as factorization // MIT Laboratory for Computer Science Technical Report, LCS/TR-212.1979. 16 p.

Rackoff C., Simon D. Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack // J. Feigenbaum (ed.): CRYPTO'91, LNCS 576. Springer-Verlag, 1992. P. 433-444.

Reed I.S., Solomon G. Polynomial Codes Over Certain Finite Fields // SIAM Journal of Applied Math. 1960. Vol. 8. P. 300-304.

Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public key cryptosystems // Communications of the ACM 21. 1978. P. 120-126.

Shpilrain V., Ushakov A. Thompson's group and public key cryptography/ Preprint arXir: math.GR/0505487, 2005. P. 151-163.

Smith P., Lennon M. LUC: A newpublic key system // Proceedings of the IFIP TC11 Ninth International Conference on Information Security, IFIP/Sec 93. North-Holland, 1993. P. 103-117.

Williams H.C. A Modification of the RSA Public-Key Encryption Procedure // IEEE Transactions on Information Theory. 1980. Vol. IT-26. No. 6. P. 726-729.

Williams H.C. Some public-key crypto-funtions as intractible as factorization // G.R. Blakley and D.Chaum (eds): CRYPTO'84, LNCS 196. Springer-Verlag, 1985. P. 66-70.

Рецензент статьи: доктор технических наук, профессор Института радиоэлектроники и информационных технологий Уральского федерального университета Л.Г. Доросинский.